by Bradley Barth, Senior Reporter
July 18, 2017

Hacker steals $7 million in Ethereum cryptocurrency after compromising start-up's token sale

A mysterious cyberthief made off with $7 million in the cryptocurrency Ethereum on Monday after hacking a virtual currency trading platform during its Initial Coin Offering and inserting a malicious address where digital investors were tricked into sending their funds.

The platform provider, a blockchain tech startup called CoinDash, disclosed in an online statement that more than 2,000 investors unknowingly sent their virtual money to the hacker, for a total of roughly 37,000 Ethereum, which equates to around $7 million. The cyberattack occurred immediately after CoinDash publicly launched its ICO token sale on July 17, the company noted.

In response, CoinDash has launched a forensic investigation, contacted law enforcement, and intends to credit victims with tokens as if they had actually sent their investments to the correct address. "We are currently gathering information regarding each for the attack victims and will release the complete list for our contributors and community review shortly," CoinDash said in the statement, attributed to co-founders Alon Muroch and Adam Efrima, and the CoinDash team.

"The only way now is to move forward. The company's vision is intact and the products we are developing are still in high demand (even more so now)," the statement continues. "Such malicious attacks will not divert us from developing a product that will make crypto investments more accessible to the public."

A 15-minute private token private involving whitelisted investors was not affected.

Although cryptocurrencies and their corresponding blockchain technologies have garnered a reputation for transactional security and privacy, incidents like this one also demonstrate that such innovations have also introduced a viable new attack vector -- one in which cybercriminals also benefit from anonymity.

“The fact that this is done with a cryptocurrency wallet ID makes it very effective, as it will make it much harder to trace the criminals, due to the anonymity provided by the algorithms behind Ethereum," said Ben Herzberg, security group research manager at cybersecurity firm Imperva. "However, similar techniques are used for other types of cybercrime as well, including altering web content for other use-cases such as site defacement, attempts to infect clients with malware, attempts to gain credentials, and more.”

"The adoption of cryptocurrencies introduces a wealth, literally, of opportunities for financial systems. It also introduces a number of risks, however, and exposure to how these platforms may be exploitable by attackers is one of them," said Scott Crawford, information security research director, at 451 Research, in an email interview.

Crawford suggested that cryptocurrency adoption rates could be affected if more incidents like the CoinDash hack occur. "While dramatic swings in cryptocurrencies have not been unheard of up to now, the way they respond to these risks should be expected to directly affect confidence in them as means of currency and exchange," Crawford said. "As with cryptography generally in the past, it's not the security of the algorithms of blockchain itself per se that should raise concerns as much as the way it is implemented. If attackers can figure out how to defeat the system, regardless of the security of its components or foundations, those issues will have to be resolved to the market's satisfaction before we should expect to see wider adoption."

"Many users, fooled by investors and so-called serial entrepreneurs, blindly believe that blockchain, particularly crytocurrencies, can make a digital revolution and provide an "unbreakable" security. Unfortunately, this assumption is wrong and leads to a very dangerous feeling of false security," said Ilia Kolochenko, CEO of High-Tech Bridge. "Blockchain technology can assure a very high level of data integrity, but we need to remember the numerous intertwined layers of modern technology stack, where one breached system or host can put the entire structure at risk."

"Victims of this hack will quite unlikely get their money back as, technically speaking, it's virtually impossible. Moreover, law enforcement won't be able to help either in this case, except if it is an insider attack that can be investigated and prosecuted," Kolochenko said.

Chris Pierson, general counsel and chief security officer of payment security company Viewpost, said that the CoinDash hack demonstrates not only that virtual currency companies must practice responsible security, but also that financial regulation may be necessary in this emerging market to ensure proper accountability.

"In the present case, there appears to have been some vulnerability that allowed a fundamental change to a payment address which could have been addressed by proper vulnerability scanning or secure development practices," said Pierson. Furthermore, "Since these currencies remain unregulated, there is little recourse for affected persons to get their money back, file a complaint, [or] have a regulator on the hook for the governance or oversight of the practices of the company or its risks."

"Essentially, the unregulated nature of cryptocurrency and lack of cybersecurity in this case presented a perfect storm for the affected site and its customers."

Topics:

- Cybercrime

Related Articles

Cybercriminals using phishing scams to steal cryptocurrencies

BY Doug Olenick Jun 14, 2017

Copycat attacks threaten survival of ethereum cryptocurrency

BY Greg Masters Jun 22, 2016

Ethereum cryptocurrency breach affects 16K

BY Robert Abel Dec 20, 2016

Most read on SC

- 167 Applebee's locations across 15 states hit with POS breach
- Recently patched Flash vulnerability spotted in massive malspam campaign
- Spring break vulnerability jeopardizes Pivotal Spring projects
- GitHub rides out record-breaking DDoS attack that leveraged memcached servers
- Equifax breach worse than thought, consumers affected now total 147.9M

Get SC Media delivered to your inbox

- ☑ Whitepaper of the Day
- ☑ Newswire
- ☑ Buzz

Enter your email address | United States ▼ | SIGN UP

SC Media arms cybersecurity professionals with the in-depth, unbiased business and technical information they need to tackle the countless security challenges they face and establish risk management and compliance postures that underpin overall business strategies.

USER CENTER

About

Contact

Advisory Board

Meet the team

Subscribe

Editorial Calendar

Executive Insight submissions

PRODUCT REVIEWS

About/Contact

FAQ

Reprints

OTHER

Privacy Policy

Terms & Conditions

MORE SC SITES

RISKsec

SC

SC awards

SC events

Follow SC Media